REMARKS

The Office Action dated January 5, 2009, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Status of the Claims

Claims 18, 30 and 31 have been amended to more particularly point out and distinctly claim the subject matter of the invention. No new matter has been added. Claims 1-9, 11-20, 22-25 and 27-34 are currently pending in the application and are respectfully submitted for consideration.

Improper Finality - Applicants' Amendments did not Necessitate New Rejection

The Office Action alleged on page 10 that "Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.**" However, Applicant's amendments did not necessitate the new grounds of rejection, as will be discussed below.

In the previous Office Action of July 24, 2008 (hereinafter the "previous Office Action"), all of the pending claims were rejected as allegedly being unpatentable over Bruck et al. (U.S. Patent No. 6,691,165) in view of Syvanne (U.S. Publication No. 2002/0157018) and further in view of McLaughlin et al. (U.S. Publication No. 2002/0165929). Independent claim 1 recites, in part, determining "whether the network management operations on the cluster, including said at least two devices, were applied correctly, and when the network management operations were not applied correctly, the

processor is configured to roll back to a successful configuration", and independent claims 9, 18, 24, 30 and 31, which each have their own scope, recite similar features. The previous Office Action conceded on page 3 that Bruck et al. fails to teach these features. Rather, the previous Office Action relied on paragraph [0012] of Syvanne to allegedly cure these deficiencies of Bruck et al. Applicants traversed the rejection with respect to Syvanne without amending the features of claim 1 alleged to by taught by Syvanne.

In the outstanding Office Action, the rejection based on Bruck et al., Syvanne and McLaughlin et al. was withdrawn and a new rejection was issued that essentially substituted Sato for Syvanne. Because the above-recited features of independent claim 1 were not amended in the previous Response filed October 14, 2008, amendments by Applicants **cannot** have necessitated the substitution of Sato in place of Syvanne. Hence, the outstanding Office Action **cannot** be made final.

Accordingly, the finality of the outstanding Office Action is improper and it is respectfully requested that the finality thereof be withdrawn.

Rejection under 35 U.S.C. § 103

Claims 1-9, 11-20, 22-25 and 27-34 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Bruck et al. in view of Sato (U.S. Patent No. 7,277,935) and further in view of McLaughlin et al. (U.S. Publication No. 2002/0165929). The Office Action took the position on pages 2-7 that the combination of Bruck et al., Sato and McLaughlin et al. teaches all of the features of the rejected

claims. Applicants respectfully traverse the rejection. Reconsideration of the claims is respectfully requested.

Independent claim 1, from which claims 2-8 and 27 depend, recites a system including a network interface configured to communicate with nodes in a cluster and a configuration subsystem operationally coupled to a remote management broker. The remote management broker is configured to distribute information between the nodes in the cluster. The system also includes a processor configured to access the cluster from a single-point, obtain information relating to at least two devices within the cluster, present the information to a user and determine network management operations to perform on the cluster. The processor is also configured to apply a configuration lock to prevent other applications from performing network management operations on the at least two devices within the cluster and to perform the determined network management operations and to determine whether the network management operations on the cluster, including the at least two devices, were applied correctly. When the network management operations were not applied correctly, the processor is configured to roll back to a successful configuration.

Independent claim 9, from which claims 11-17 and 28 depend, recites a method including accessing a cluster from a single-point, obtaining attributes relating to at least two devices within the cluster, presenting the attributes to a user and receiving input from the user relating to the attributes and determining network management operations to perform on the cluster based on the received input. The method also includes applying a

configuration lock to prevent other applications from performing network management operations on the at least two devices within the cluster and performing the determined network management operations on the cluster. The method further includes determining whether the network management operations on the cluster, including the at least two devices, were applied correctly. When the network management operations were not applied correctly, the method further includes rolling back to a successful configuration.

Independent claim 18, from which claims 19, 20, 22, 23 and 29 depend, recites a computer program embodied on a computer readable storage medium configured to control a processor to perform a process, including accessing a cluster from a single-point, obtaining attributes relating to at least two devices within a cluster from a single-point and presenting the attributes to a user and receiving input relating to the attributes from the user. The process also includes determining network management operations to perform on the cluster based on the received input, applying a configuration lock to prevent other applications from performing network management operations on the at least two devices within the cluster and performing the determined network management operations on the cluster. The process further includes determining whether the network management operations on the cluster, including the at least two devices, were applied correctly, and when the network management operations were not applied correctly, rolling back to a successful configuration.

Independent claim 24, from which claim 25 depends, recites an apparatus including obtaining means for obtaining attributes relating to at least two devices within a

cluster from a single-point, providing means for providing the attributes to a user, receiving means for receiving input relating to the attributes from the user, determining means for determining network management operations to perform on the cluster based on the received input and distributing means for distributing the network management operations to the devices within the cluster. The apparatus also includes first applying means for applying a configuration lock to prevent other applications from performing network management operations on the at least two devices within the cluster and second applying means for applying the network management operations to the devices within the cluster. The apparatus further includes determining means for determining whether the network management operations on the cluster, including the at least two devices, were applied correctly, and when the network management operations on the cluster were not applied correctly, rolling back to a successful configuration.

Independent claim 30 recites an apparatus including accessing means for accessing the cluster from a single-point, obtaining means for obtaining attributes relating to at least two devices within the cluster and presenting means for presenting the attributes to a user and receiving input from the user relating to the attributes. The apparatus also includes operation determining means for determining network management operations to perform on the cluster based on the received input, applying means for applying a configuration lock to prevent other applications from performing network management operations on the at least two devices within the cluster and performing means for performing the determined network management operations on the cluster. The apparatus further

includes correction determining means for determining whether the network management operations on the cluster, including the at least two devices, were applied correctly, and when the network management operations were not applied correctly, rolling back to a successful configuration.

Independent claim 31, from which claims 32-34 depend, recites an apparatus including a processor configured to access a cluster from a single-point, obtain attributes relating to at least two devices within the cluster and present the attributes to a user and receive input from the user relating to the attributes. The processor is also configured to determine network management operations to perform to the cluster, apply a configuration lock to prevent other applications from performing network management operations on the at least two devices within the cluster and perform the determined network management operations. The processor is further configured to determine whether the network management operations on the cluster, including the at least two devices, were applied correctly, and when the network management operations were not applied correctly, the processor is configured to roll back to a successful configuration.

As will be discussed below, Bruck et al., Sato and McLaughlin et al., both individually and in combination, fail to teach or suggest all of the features of the presently pending claims.

Bruck et al. generally discusses "a scalable, distributed, highly abailable, load balancing server system having multiple machines functioning as a front server layer between the network and a back-end server layer having multiple machines functioning

as Web file servers, FTP servers, or other application servers" (column 2, lines 42-47). "The operation of the servers on both layers is monitored, and when a server failure at either layer is detected, the system automatically shifts network traffic from the failed machine to one or more operational machines, reconfiguring front-layer servers as needed without interrupting operation of the server system" (column 2, lines 49-54, of Bruck et al.). "The front layer machines perform their operations without breaking network communications between clients and servers, and without rebooting of computers. In this way, the system [allegedly] provides reliable network communication in a scalable load balancing solution for server farms" (column 2, lines 63-67, of Bruck et al.).

Sato generally discusses "management of a communications apparatus" and the discussion thereof is allegedly applicable "to initial settings by a management device on a network device such as a hub and a router connected to a network" (see column 1, lines 7-11). A method as discussed in Sato may include:

> providing, via one or more interconnecting devices connected to a network, an address of a target device which is connected to one of the interconnecting devices, or a port identifier for identifying a port of the target device which is connected to one of the interconnecting devices via a port of one of the interconnecting devices, for a management device that is connected to the network so as to manage the target device; and the management device managing the target device based upon the provided address. According to this management method, the management device manages the target device based upon the address or port identifier provided from the interconnecting device. This allows the address or port identifier to be automatically provided from the interconnecting device to the management device, and thus facilitates the management including initial configuration.

(Column 3, lines 1-17).

McLaughlin et al. generally discusses "the allocation, retention, and release of control of a programmable switch in a switched network to allow maintenance to be performed thereon" (paragraph [0005]). "[A] mechanism is provided that allows for synchronization of online maintenance of the firmware and configuration files in the programmable switch components of a network. At the same time, the ability to direct that maintenance remains distributed among the nodes of the network" (paragraph [0012], of McLaughlin et al.).

Independent claim 1 recites, in part, determining "whether the network management operations on the cluster, including said at least two devices, were applied correctly, and when the network management operations were not applied correctly, the processor is configured to roll back to a successful configuration." Independent claims 9, 18, 24, 30 and 31, which each have their own scope, recite similar features. The Office Action conceded on page 3 that Bruck et al. fails to teach these features. Rather, the Office Action relied on Fig. 13 and column 16, lines 10-17, of Sato to allegedly cure these deficiencies of Bruck et al. Applicants respectfully submit that Sato also fails to teach or suggest these features.

The cited section of Sato discusses that:

> TFTP transmits and receives mainly configuration information and firmware of the network device 60 in the form of a file. For example, the configuration information is collected as a file, and if the network device 60 fails, the file is transmitted by return and used when the original configuration information should be restored. Under HTTP, HTML (Hypertext Markup Language) documents are transmitted and received between the management device 10 and the network device 60.

The above discussion does not occur in the context of a cluster. Thus, in Sato, a non-clustered management device may collect configuration information (the **original** configuration information) as a file and if a network device fails, the file is transmitted to the network device and used to restore the original configuration information in the firmware of, for example, a network switch.

On the other hand, claim 1 recites that "when the network management operations were not applied correctly, the processor is configured to roll back to a **successful configuration**." In other words, when network management operations are incorrect, the configuration is rolled back to a previous, successful configuration. Thus, claim 1 recites rolling back to a previous, successful configuration, whereas Sato merely discusses restoring parameters of an initial firmware configuration.

As discussed on page 1, lines 24-27, of the present specification, "[o]ne problem is that it is difficult to maintain identical configurations of the Network Management features on all devices within a cluster. In addition, errors in the configuration of one device, or incompatible configurations among the devices, may render a particular NM feature inoperable." By rolling back to a successful configuration, some embodiments of the present invention have the advantage of being able to maintain successful configurations that occurred after the initial implementation of the cluster, which allows better management and adaptability of the cluster throughout its lifetime. Such features are simply absent from, and such advantages simply cannot be achieved with, the system

discussed in Sato. Further, nothing is cited or found in McLaughlin et al. that overcomes the above deficiencies of Bruck et al. and Sato.

Further, Applicants respectfully submit that the combination of Sato with Bruck et al. and McLaughlin et al. is improper. Sato generally discusses managing a network device, but does not discuss such management in the context of a cluster. In fact, the word "cluster" does not appear anywhere in Sato. As such, Applicants do not believe that a person of ordinary skill in the art would be motivated to consult a non-clustered system, such as that in Sato, when attempting to modify a clustered system, such as that in Bruck et al. and McLaughlin et al. Applicants submit that management in a clustered environment differs from management in a non-clustered environment, and that it would likely cause problems for the cluster in many implementations if a failed device was restored to an initial firmware configuration, as discussed in Sato. Such a solution would likely be static and inflexible, lacking usefulness in real world applications.

Claims 2-8, 11-17, 19, 20, 22, 23, 25, 27-29 and 32-34 depend from independent claims 1, 9, 18, 24 or 31 and add further features thereto. Thus, the arguments above with respect to the independent claims also apply to the dependent claims.

Per the above, Bruck et al., Sato and McLaughlin et al., both individually and in combination, fail to teach or suggest all of the features of the above-rejected claims under 35 U.S.C. § 103(a). Accordingly, it is respectfully submitted that the rejection is overcome and respectfully requested that the rejection be withdrawn.

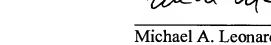
Conclusion

For at least the reasons presented above, it is respectfully submitted that claims 1-9, 11-20, 22-25 and 27-34, comprising all of the currently pending claims, patentably distinguish over the cited art. Accordingly, it is respectfully requested that the claims be allowed and the application be passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, Applicants' undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, Applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Michael A. Leonard II
Attorney for Applicants
Registration No. 60,180

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Vienna, Virginia 22182-6212
Telephone: 703-720-7800
Fax: 703-720-7802
MAL:jf